Prelude-LML - Bug #331

RULE CISCO-ROUTER UNRECOGNIZED

11/04/2008 09:58 PM -

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.15		
Resolution:	invalid		

Description

The following rule is not recognized:

The log is the following:

Nov 3 08:36:08 10.129.192.205 81: Nov 3 08:42:45 Caracas: %SEC-6-IPACCESSLOGDP: list prueba_access_in denied icmp 10.10.10.1 -> 10.12.14.3 (3/1), 3 packets

My regex is the following:

```
regex=%SEC-6-IPACCESSLOGDP: list (\w+) denied (icmp) ([\d\.]+)\s+\-\>\s+([\d\.]+)\s+\(([\d\/]+)\), (\d+); \
classification.text=Packet denied; \
classification.reference(0).origin=vendor-specific; \
classification.reference(0).meaning=cisco_id; \
classification.reference(0).name=%SEC-6-IPACCESSLOGDP; \
classification.reference(0).url=http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_system_message_guide_chapte$
id=505; \
revision=2; \
analyzer(0).name=Router; \
analyzer(0).manufacturer=Cisco; \
analyzer(0).class=Router; \
assessment.impact.completion=failed; \
assessment.impact.type=other; \
assessment.impact.severity=medium; \
assessment.impact.description=Someone tried to bypass access-list #$1; \
source(0).node.address(0).category=ipv4-addr; \
source(0).node.address(0).address=$3; \
source(0).service.port=$4; \
source(0).service.iana_protocol_name=$2; \
target(0).node.address(0).category=ipv4-addr; \
target(0).node.address(0).address=$4; \
target(0).service.port=$6; \
last
```

Can you help me? because the regex is matched with the Log..

History

#1 - 11/05/2008 09:53 AM - Yoann VANDOORSELAERE

- Status changed from New to Closed

- Resolution set to invalid

Please use the prelude-user mailing list for help on writing LML rules. Additionally, the current LML ruleset already contain similar rules as this one, that might easily be modified to handle your log.

#2 - 04/29/2009 12:21 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude-LML

- Category deleted (4)

- Target version deleted (93)